What is claimed is:

CLAIMS

1. A method for digitally signing a message, the method comprising:

providing a message digest (M_X, M_Z);

providing a modulus N;

providing a number V in the ring Z_N, wherein for another number S in the ring Z_N, $V \cdot S^2 = 1$ in Z_N;

solving the equation $(M_x + x)^2 - V \cdot y^2 = 4 \cdot (M_z + z)$ in Z_N to produce x, y, and z; and

assigning SIG as the signature of (M_X, M_Z), wherein SIG comprises (x,y).

2. The method according to claim 1 and wherein SIG comprises (x,y,z).

3. The method according to claim 1 and wherein the solving comprises the following:

a) choosing α and β in Z such that $0 \le \alpha < \beta < 2^{k-1}$ and $\gcd(\alpha, \beta) = 1$ in Z;

b) choosing γ in Z such that $2^{n-k-1} \le \gamma < 2^{n-k}$ and $\beta \mid (\alpha \cdot N + \gamma)$ in Z;

c) setting R equal to $(\alpha \cdot N + \gamma) / \beta$ in Z;

d) setting T equal to $-(M_z \cdot R + M_x + R^{-1})$ in Z_N;

e) if $\beta = 1$ or $T < 8 \cdot \gamma$ (in Z), setting U and W equal to 0 and continuing with step k;

f) setting D equal α^{-1} in Z_β;

g) setting A equal to N / β in Z;

h) setting B equal to $(T - 8 \cdot \gamma) / A$ in Z;

i) setting U equal to $B \cdot D$ in Z_β;

j) setting W equal to $U \cdot R$ in Z_N;

k) setting C $(T - W) / \gamma$ in Z;

l) setting z equal to $U + \beta \cdot C$ in Z_N;

m) setting x equal to $T - z \cdot R$ in Z_N; and

n) setting y equal to $S \cdot (x + M_x + 2 \cdot R^{-1})$ in Z_N,

thereby producing x, y, and z.

4. The method according to claim 3 and also comprising:

providing a trusted computation device and a non-trusted computation device,

wherein step d) comprises performing a computation in the non-trusted computation device.

5. The method according to claim 4 and wherein the computation in the non-trusted computation device comprises a computation of R^{-1}.

6. The method according to claim 5 and wherein the computation in the non-trusted computation device is protected from tampering by performing a blinding method in the trusted computation device.

7. The method according to claim 6 and also comprising verifying a result of the computation in the non-trusted computation device.

8. The method according to claim 3 and wherein step a) comprises screening α and β.

9. The method according to claim 8 and wherein the screening comprises reducing α and β modulo 210.

10. The method according to claim 9 and wherein the reducing α and β modulo 210 comprises:

computing gcd(210, (α mod 210), (β mod 210)) to produce a result; and

rejecting α and β and choosing another α and β if the result is not equal to 1.

11. The method according to claim 1 and wherein the solving comprises the following:

a) setting α equal to 0;

b) setting $\beta = 1$;

c) choosing γ such that $2^{n-k-1} \leq \gamma < 2^{n-k}$;

d) setting T equal to $-(M_z \cdot \gamma + M_x + \gamma^{-1})$ in Z_N;

e) setting z equal to T / γ in Z;

f) setting x equal to $T - z \cdot \gamma$ in Z_N; and

g) setting y equal to $S \cdot (x + M_x + 2 \cdot \gamma^{-1})$ in Z_N,

thereby producing x, y, and z.

12. The method according to claim 11 and also comprising:

providing a trusted computation device and a non-trusted computation device,

wherein step d) comprises performing a computation in the non-trusted computation device.

13. The method according to claim 12 and wherein the computation in the non-trusted computation device comprises a computation of γ^{-1}.

14. The method according to claim 13 and wherein the computation in the non-trusted computation device is protected from tampering by performing a blinding method in the trusted computation device.

15. The method according to claim 14 and also comprising verifying a result of the computation in the non-trusted computation device.

16. A message signer for digitally signing a message based on a message digest (M_X, M_Z), a modulus N, and a number V in the ring Z_N, wherein for another number S in the ring Z_N, $V \cdot S^2 = 1$ in Z_N, the message signer comprising:

a solver for solving the equation $(M_x + x)^2 - V \cdot y^2 = 4 \cdot (M_z + z)$ in Z_N to produce x, y, and z; and

a signature assignor for assigning SIG as the signature of (M_X, M_Z), wherein SIG comprises (x,y).